Sistemas Distribuídos 2016/2017

3ª Parte - Relatório de Segurança

Professor Naércio Magaia

Turno de 2ª feira, às 11h

Grupo A45 - https://github.com/tecnico-distsys/A45-Komparator

Rafael Belchior 80970	João Trindade 80805	Pedro Gomes, 81534

Lisboa, 5 de Maio de 2017

A nossa política de segurança

Quem proteger? Assegurar a privacidade e confidencialidade do cliente.
Quem são os atacantes? Não sendo atacantes, os professores irão verificar se o código cumpre os requisitos de segurança.
Quais os ataques? Os ataques podem ser variados: ataque brute-force, ataque do tipo man-in-the-middle, ataque do aniversário, e outros eventuais tipos de ataque.
Quais os procedimentos e mecanismos de proteção que podem impedir os ataques considerados? A implementação de um mecanismo de encriptação, baseado em chaves assimétricas vai permitir proteger a confidencialidade do cliente. O uso de assinaturas digitais, com o apoio da autoridade de certificação (CA), vai permitir prevenir ataques do género man-in-the-middle (e possivelmente o ataque do aniversário).

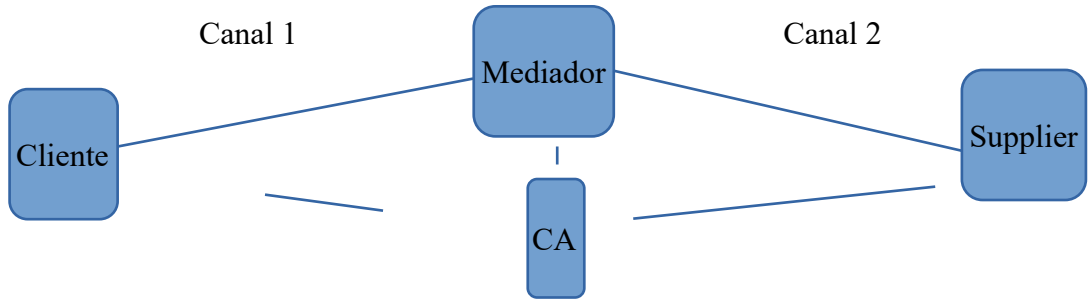


Figura 1- Esquema simplificado da solução de segurança

Nota: A obtenção das chaves privadas é feita de forma local, através das keystores (ficheiros .jks), disponibilizados. A obtenção das chaves públicas de uma entidade é feita através da leitura do certificado que lhe corresponde. Os certificados são obtidos via serviço CA, alojado na RNL. Quando obtemos um certificado, guardamo-lo num hashmap, de modo a reduzir o número de coneções com a CA. A chave pública da CA é conhecida por todos os participantes.
Em todo o momento, cada entidade sabe o seu próprio nome, através do uso do padrão de desenho singleton. Cada processo tem um objeto singleton a ele associado, que o identifica.

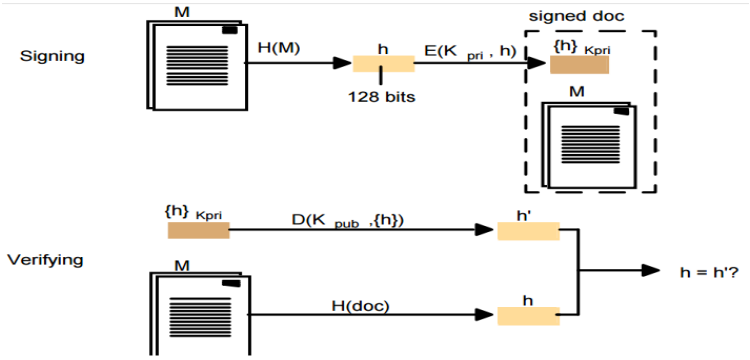
Requisitos:

O valor do cartão de crédito deve ser enviado do cliente para o mediador de forma a que apenas este último o consiga ler (canal 1 da Figura 1).

O requisito pedido é confidencialidade, obtida através do estabelecimento de um canal seguro entre o cliente e o mediador. A informação sensível a ser protegida é o número do cartão de crédito. Quando se procede a uma compra, o cliente envia o número de cartão de crédito ao mediador. Este número deve ser cifrado antes da mensagem ser enviada. Assim, impedem-se fugas de informação, nomeadamente do número do cartão de crédito.

Para cifrar este número, acedemos ao body da SOAP message, encriptando o conteúdo da tag "creditCardNr", usando uma chave assimétrica. O número do cartão de crédito é cifrado com a chave pública do mediador. Quando a mensagem é recebida por este, o conteúdo cifrado presente na tag "creditCardNr" é decifrado com a chave privada do mediador. Deste modo, se a mensagem for intercetada, o número de cartão de crédito que for descoberto estará encriptado, e, portanto, inacessível.

As mensagens trocadas entre o mediador e os fornecedores devem estar autenticadas e não devem poder ser repudiadas à posteriori pelo seu emissor (canal 2 da Figura 1).
As assinaturas digitais permitem prevenir não só o tampering, como também assegurar autenticidade, integridade e não repudiação à posteriori pelo seu emissor (ou seja, é possível provar que foi o emissor que enviou a mensagem em questão).



Conseguimos concretizar o objetivo através de duas etapas:

No outbound: sobre o header + body da mensagem SOAP, aplicar a função de hashing e encriptar o resultado, obtendo-se o Digest. Criar uma tag no header da mensagem SOAP, chamada "messageDigest" e inserir lá o Digest.

No inbound: Retirar a tag "messageDigest" do header da mensagem SOAP. Obter a chave pública do sender da mensagem. Aplicá-la ao Digest, obtendo-se o resultado da aplicação da fução de hash à mensagem (H(M)). Aplicar a função de hashing (é pública e conhecida) à mensagem, e verificar se é igual a H(M). Se for, a mensagem é autentica, e veio do sender. Caso contrário, pode ter havido modificação da mensagem, entre o sender e o receiver. O esquema acima resume a descrição feita.

As mensagens devem ser protegidas para garantir a sua frescura, i.e., devem prevenir ataques por repetição feitos por um agente malicioso que reenvia mensagens enviadas anteriormente por um agente legítimo (presente em todos os canais).
Adicionamos um timestamp ao header de cada mensagem. Esta solução permite que a mesma mensagem não seja enviada num intervalo de tempo arbitrário, como, por exemplo, três segundos. O elemento da mensagem SOAP que contém o timestamp chama-se "TimeStamp".
Esta solução é simples de implementar e, para o contexto do projeto, acreditamos que é suficiente. No entanto, o uso de nonces é uma melhor solução, já que a solução anterior não consegue lidar com os casos em que se enviam mensagens repetidas num intervalo de tempo inferior ao estipulado. Os nonces são números gerados aleatoriamente, que permitem identificar univocamente uma mensagem. Esta solução tem, pelo menos, um problema. Ao ter de se guardar n destes números, e ao ter de se fazer O(n) comparações por cada mensagem, temos um problema de escalabilidade e eficiência. Consideramos que a solução ideal seria uma solução híbrida. Usar-se-iam os nonces para evitar mensagens repetidas, combinado com um timer, para se eliminarem os nonces mais antigos.

Esquema das mensagens SOAP (pedido e resposta)

Mensagem capturada do MediatorHandler. Verifica-se que o "creditCarNr" é encriptado com sucesso.

```
-------LOGGING OUTBOUND-----
----------------------------
 SOAP message:
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"><SOAP-ENV:Header/><S:Body><ns2:buyCart xmlns:
ns2="http://ws.mediator.komparator.org/"><cartId>car</cartId><creditCardNr>4024007102923926</creditCardNr></ns2:buyCart></S:Body></S:Envelope>
AddHeaderHandler: Handling message.
AddHeaderHandler: Handling message.
[2017-05-05T16:09:49.224] ----------------------------
-------LOGGING OUTBOUND-----
----------------------------
 SOAP message:
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"><SOAP-ENV:Header/><S:Body><ns2:buyCart xmlns:
ns2="http://ws.mediator.komparator.org/"><cartId>car</cartId><creditCardNr>icgy6k1BQJPDr9WzfuqyTNmmvi8Js0/xg1zI9NPa2reJmhh/w0yFYycbyWk32PVxe/vR5/+xui0R6GyBkSLTHiS3I2DM2
S1AgXtlXDGUxRymiqveYuYr+5yRrh2JTrkCMgXQrGf8S7lG/xTv7b/e/CKtOsnBxr1gJYPf0FN7tuxBYFPGya1LAtmos4dUb/KRKJaQUS54KcBfclXi4C3+32ocYFshqoZR5Z0MtYtPlTkK9oIcgpzoDbeZAHpS/uYP/HY9W
xnHGwvRvX4IDHabCTpVFaQsZect/V3DHXqFIUnt09IEAC4ePdfX7CqSoIpYnvkmeKIOLR1e7WBbpXlMsg==</creditCardNr></ns2:buyCart></S:Body></S:Envelope>
[2017-05-05T16:09:49.555] ----------------------------
```

Mensagem capturada do SupplierHandler. Verifica-se que é adicionada a tag da assinatura, "messageDigest" e o tag "Timestamp".

```
----------------------------
        ----LOGGING OUTBOUND----
----------------------------
 SOAP message:
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"><SOAP-ENV:Header/><S:Body><ns2:pingResponse x
mlns:ns2="http://ws.supplier.komparator.org/"><return>Hello client from Supplier</return></ns2:pingResponse></S:Body></S:Envelope>
[2017-05-05T18:08:38.233] intercepted OUTbound
----------------------------
        ----LOGGING OUTBOUND----
----------------------------
 SOAP message:
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"><SOAP-ENV:Header><timeStamp:TimeStamp xmlns:t
imeStamp="http://demo">2017-05-05T18:08:37.811</timeStamp:TimeStamp><d:messageDigest xmlns:d="http://demo">De0gxQhCp6904IDiNJr/8JUW83GTBD0F0xdoRBGTlkJ2EctlZKRSJgz0Q/oHz
8zbmbyJRBctYqXxdgBs4qSsNcDmQ+ZPvr2VOy9YXnAym90deoh30W802BZEenV57TGY59grtFGEnhRC42BCJxwd6+RS6v3ocnclTIlDdZ9/mNgQd/PG7urq0JbGfuHHRdpSq1j7aBP/O7DHA2MXYG/NsFQLgMbbrKVM0nxlG
wy7v2FXXTn/JvBJzuX449h1lp+uQoHIdF1kPaywGcY2RJonztupkg+MZvkzUTZJYLILXMFqHlJvwf74/oONDnDx68BY95etXQGToNQTA82KC3zFbw==</d:messageDigest></SOAP-ENV:Header><S:Body><ns2:ping
Response xmlns:ns2="http://ws.supplier.komparator.org/"><return>Hello client from Supplier</return></ns2:pingResponse></S:Body></S:Envelope>
```